M-10-127

UNDER SEAL

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK
- - - - - - - - - - - - - - - - - - - -X
IN THE MATTER OF THE APPLICATION FOR A SEARCH WARRANT FOR: THE CONTENTS OF ELECTRONIC COMMUNICATIONS SENT OR RECEIVED OVER THE EMAIL ACCOUNT egsys@aol.com, SERVICED BY AOL LLC, SUBSCRIBED TO IN THE NAME OF EDWARD GRODSKY, OCEAN SIDE, NEW YORK IN ELECTRONIC STORAGE OR IN A REMOTE COMPUTING SERVICE BY AOL LLC, 22000 AOL WAY, DULLES, VA 20166
- - - - - - - - - - - - - - - - - - - -X
EASTERN DISTRICT OF NEW YORK, SS:

AFFIDAVIT IN SUPPORT OF SEARCH WARRANT
(T. 18 U.S.C. § 2703)

SHELDON TANG, being duly sworn, deposes and says that he is a Special Agent with the Internal Revenue Service ("IRS"), duly appointed according to law and acting as such.

Upon information and belief, there is probable cause to believe that there is located in the PREMISES KNOWN AS ELECTRICAL MAIL ADDRESS "EGSYS@AOL.COM" (the "PREMISES") controlled by the web-based electronic mail service provider America Online ("AOL" or the "Provider") subscriber/profile information, email transmission information, subject headings, to/from information, folders and email content (including all of the foregoing for deleted messages) as described more fully in Attachment A, for the dates between and including January 1, 2008 ST to the present, which constitutes evidence, fruits and instrumentalities of violations of Title 18, United States Code, Sections 371, 1341, 1343, 1349 and 1956.

(Title 18, United States Code, Sections 371, 1341, 1343, 1349 and 1956)

1. I am a Special Agent of the Internal Revenue Service ("IRS"), duly appointed according to law and acting as such. I have been a Special Agent for approximately five and one half years. During my tenure with the IRS, I have participated in many fraud and money laundering investigations, which have included, among other investigative techniques, the use of physical surveillance, execution of search warrants, consensual recordings of individuals associated with fraud and money laundering schemes and debriefing of cooperating witnesses and other informants.

2. I make this Affidavit in support of the application of the United States of America for the issuance of a warrant to search the PREMISES controlled by the web-based electronic mail service provider, AOL. Based on information and belief, there is probable cause to believe that located in the PREMISES is evidence relating to the participation of EDWARD GRODSKY and others, in a ~~conspiracy~~ ST scheme to commit conspiracy, mail fraud, wire fraud and money laundering in violation of Title 18, United States Code, Sections 371, 1341, 1343, 1349 and 1956, and other items described in Attachment A, appended hereto.

3. The information contained in this affidavit is based, in part, on personal knowledge arising from my participation in this investigation, and, in part, on information and belief. The sources of my information and belief include, among other things: (a) statements made to me, and information provided to me by Special Agents of the IRS and Postal Inspectors

of the United States Postal Inspection Service assigned to the investigation (collectively, "Special Agents of the Investigating Agencies"), confidential informants and other witnesses; and (b) my review of various documents and records. Where the statements of others or the contents of documents and records are related herein, they are related in substance and in part, and not verbatim, unless indicated otherwise. Since this affidavit is being submitted for a limited purpose, I have not set forth each and every fact that I know concerning this investigation. Rather, I have set forth only those facts that I believe are necessary to establish probable cause for the search warrant sought herein.

APPLICABLE DEFINITIONS

4. The following terms have the indicated meaning in this affidavit:

a. The term "computer," as used herein, is defined as set forth in Title 18, United States Code, Section 1030(e)(1).

b. The terms "records," "documents," and "materials" include all information recorded in any form, visual or aural, and by any means, whether in handmade form (including, but not limited to, writings, drawings, paintings), photographic form (including, but not limited to, microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, photocopies), mechanical form (including, but not limited to, phonograph records, printing, typing) or electrical, electronic or magnetic form (including, but not limited to, tape recordings, cassettes, compact discs, electronic or magnetic storage devices

such as floppy diskettes, hard disks, CD-ROMs, digital video disks (DVDs), Personal Digital Assistants (PDAs), Multi Media Cards (MMCs), memory sticks, optical disks, printer buffers, smart cards, memory calculators, electronic dialers, Bemoulli drivers, or electronic notebooks, as well as digital data files and printers or readouts from any magnetic, electrical or electronic storage device).

BACKGROUND INFORMATION REGARDING THE INTERNET, COMPUTERS AND EMAIL

5. I have had both training and experience in the investigation of crimes that involve the use of computers. Based on my training, experience, knowledge, and conversations with other law enforcement agents familiar with computer crimes, I know the following:

a. The internet is a worldwide network of computer systems operated by governmental entities, corporations, and universities that connects computers and allows communications and the transfer of data and information across state and national boundaries. The term computer includes an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device. In order to access the internet, an individual computer user must subscribe to an access provider, which operates a host computer system with direct access to the Internet. The world wide web ("www") is a functionality of the

Internet which allows users of the Internet to share information;

b. With a computer connected to the Internet, an individual computer user can make electronic contact with millions of computers around the world. This connection can be made by any number of means, including modem, local area network, wireless, and numerous other methods; and

c. Electronic mail ("email") is a popular form of transmitting messages and/or files in an electronic environment between computer users. When a computer user sends an email, the email is initiated at the user's computer, transmitted to the subscriber's mail server, and then transmitted to its final destination. A server is a computer attached to a dedicated network and serves many users. An email server may allow users to post and to read messages and to communicate by electronic means.

d. An instant messenger is a computer application which allows real-time, instantaneous text communication between two or more people -- much like an oral conversation -- through a computer network, such as the Internet. People communicating in real-time through such application are said to be "instant-messaging" or "IM-ing" one another, or "chatting" with one another.

e. A "Newsgroup" is a site on the World Wide Web where any number of computer users can post messages to each other. These messages usually appear on an area of the screen

next to the user's online nickname. The name of a "Newsgroup" generally stems from the topics discussed therein.

f. In addition to sending and receiving text messages and images, an individual can use the Internet to send or receive a video clip, which generally is in the form of an mpg file. A user can also use a webcam to capture live video images and then instantaneously transmit those images via the Internet to another user to be viewed on a computer at another location.

g. An Internet Service Provider ("ISP") is an organization or commercial service that provides individuals with access to the Internet computer network. The ISP assigns each user an Internet Protocol ("IP") number or address. This IP address is a multi-digit number (for instance, 209.209.171.80) that is required for a user to gain access to websites on the Internet or transmit files to other Internet users. An ISP assigns a unique IP address to each of its users accessing the Internet.

h. The user will maintain this same IP address for the period that he is connected to the Internet; for this reason, many Internet users with cable modems or Digital Subscriber Lines ("DSL" lines) maintain an IP address for long periods of time because they maintain a constant connection to the Internet.

6. I have also learned the following about the Internet Service Provider:

a. The Provider operates email services which are available to Internet users. Subscribers obtain an account by registering on the Internet with the Provider. The Provider request subscribers to provide basic information, such as name, gender, zip code and other personal/biographical information. However, the Provider does not verify the information provided.

b. The Provider maintains electronic records pertaining to the individuals and companies for which it maintains subscriber accounts. These records include account access information, email transaction information, and account application information.

c. Subscribers to the Provider may access their accounts on servers maintained and/or owned by the Provider from any computer connected to the Internet located anywhere in the world.

d. Any email that is sent to the Provider's subscriber is stored in the subscriber's "mailbox" on the Provider's servers until the subscriber deletes the email or the subscriber's mailbox exceeds the storage limits preset by the Provider.

e. When the subscriber sends an email, it is initiated at the user's computer, transferred via the Internet to the Provider's servers, and then transmitted to its end destination. The Provider's users have the option of saving a copy of the email sent. Unless the sender of the email specifically deletes the email from the Provider's server, the

email can remain on the system indefinitely. The sender can delete the stored email message thereby eliminating it from the email box maintained at the Provider, but that message will remain in the recipient's email box unless the recipient deletes it as well or unless the recipient's account is subject to account size limitations.

f. A Provider's subscriber can store files, including emails and image files, on servers maintained and/or owned by the Provider.

g. Emails and image files stored on a Provider's server by a subscriber may not necessarily be located in the subscriber's home computer. The subscriber may store emails and/or other files on the Provider's server for which there is insufficient storage space in the subscriber's computer and/or which he/she does not wish to maintain in the computer in his/her residence. A search of the files in the computer in the subscriber's residence will not necessarily uncover the files that the subscriber has stored on the Provider's server.

h. Computers located at the Provider contain information and other stored electronic communications belonging to unrelated third parties. Accordingly, this affidavit and application for search warrant seek authorization solely to search the computer accounts and/or designated files and following the procedures described herein and in Attachment A.

STATUTORY PROVISIONS

7. Title 18, United States Code, Sections 2701 through 2711, is entitled "Stored Wire and Electronic Communications and Transactional Records Access."

a. Title 18, United States Code, Section 2703(a) provides, in part:

> A governmental entity may require the disclosure by a provider of electronic communication service of the contents of a wire or electronic communication, that is in electronic storage in an electronic communications system for one hundred and eighty days or less, only pursuant to a warrant using the procedures described in the Federal Rules of Criminal Procedure by a court with jurisdiction over the offense under investigation or equivalent State warrant. A governmental entity may require the disclosure by a provider of electronic communications services of the contents of a wire or electronic communication that has been in electronic storage in an electronic communications system for more than one hundred and eighty days by the means available under subsection (b) of this section.

b. Title 18, United States Code, Section 2703(b) provides, in part:

> (1) A governmental entity may require a provider of remote computing service to disclose the contents of any wire or electronic communication to which this paragraph is made applicable by paragraph (2) of this subsection-
>
> (A) without required notice to the subscriber or customer, if the governmental entity obtains a warrant issued using the procedures described in the Federal Rules of Criminal Procedure by a court with jurisdiction over the offense under investigation or equivalent State warrant.

> (2) Paragraph (1) is applicable with respect to any wire or electronic communication that is held or maintained on that service-
>
> (A) on behalf of, and received by means of electronic transmission from (or created by means of computer processing of communications received by means of electronic transmission from, a subscriber or customer of such remote computing service; and
>
> (B) solely for the purpose of providing storage or computer processing services to such subscriber or customer, if the provider is not authorized to access the contents of any such communications for purposes of providing any services other than storage or computer processing.

c. The government may also obtain records and other information pertaining to a subscriber or customer of an electronic communication service or remote computing service by way of a search warrant. 18 U.S.C. § 2703(c)(2). No notice to the subscriber or customer is required. 18 U.S.C. § 2703 (c)(3).

THE INVESTIGATION

8. Since approximately October of 2009, the IRS has been investigating Liberty Planning, Incorporated, an insurance agency, for possible tax fraud, mail and wire fraud and money laundering related to fraudulent life insurance policies. The IRS began its investigation when it received information about an internal fraud investigation conducted by ING Group, N.V., a life insurance company, concerning a large number of multi-million dollar life insurance policies that the company believed Liberty Planning had fraudulently induced it to issue.

9. ING is an international financial services company that sells, among other things, life insurance. Liberty Planning is a general insurance agency located in Monsey, New York.[1] ING enters into agreements with a number of licensed insurance agents, such as the agents affiliated with Liberty Planning, whom ING has approved to act as insurance agents on ING life insurance policies. Each insurance agent is supposed to find potential insureds (or other persons with an insurable interest in the insured's life, such as a close relative of the insured) who wish to purchase life policies from ING. If ING approves an insured's application for a policy, the agent receives a commission out of the premiums that the insured (or the owner of the policy on the insured's life) pays to ING. In short, the ING insurance agent is a salesman for ING life insurance policies who is compensated by commission. The investigation has uncovered facts indicating that CHAIM LEBOVITS, MOSES SCHLESINGER, a number of agents associated with Liberty Planning and others, including EDWARD GRODSKY, have been defrauding ING and other life insurance companies by submitting applications containing false statements to induce the insurance companies to enter into life insurance

---

[1]CHAIM LEBOVITS is listed on the Liberty Planning letterhead as the Vice-President of Liberty Planning and, based upon my understanding to date as a result of speaking with an ING investigator, LEBOVITS acts as the company's General Agent who is in charge of all of the other agents. In the report of ING's internal investigation, ING described MOSES SCHLESINGER as the Office Manager of Liberty Planning. SCHLESINGER reported on his passport application that he is Office Manager of Liberty Planning.

contracts. Specifically, Liberty Planning has submitted to ING and other insurance carriers numerous fraudulent applications to purchase multi-million dollar life insurance policies on elderly persons which the insurance companies would not have issued if they had known that: (1) the insureds' net worths were vastly overstated; (2) the insureds were not going to pay the enormous premiums on the policies but, instead, unrelated investors were going to pay the premiums; and (3) the intent of the applicants when they purchased the policies was to resell the policies at a profit on the open market after two years, instead of providing the insureds' families with financial protection in the event of the insureds' premature deaths. The applications were approved and life insurance policies were issued. The premiums on the life insurance policies were paid by mail and by interstate wire transfer.

10. ING, during its internal fraud investigation, initially identified policy applications submitted by Liberty Planning to ING on at least fifteen different elderly insureds (referred to collectively as the "Fifteen Insureds," when speaking about these fifteen elderly persons, and referred to collectively as the "Fifteen Insureds' Applications," when speaking of the insurance applications submitted by Liberty Planning to ING on behalf of these Fifteen Insureds). The Fifteen Insureds' Applications sought (and ultimately were granted) ING life insurance policies that totaled over $135,000,000. Subsequent to issuing these policies, ING

investigated the Fifteen Insureds' Applications and, as a result, it terminated for cause its relationship with the five Liberty Planning agents (the "Five Agents") responsible for submitting the Fifteen Insureds' Applications. The "cause" that ING believed that it had for terminating the Five Agents was "misconduct," to wit, the Five Agents' misconduct in submitting applications for stranger owned life insurance policies to ING[2] containing significant incorrect and/or misleading information. None of the Five Agents cooperated with ING's investigation.[3] On some of the Fifteen Insureds' Applications, Liberty Planning submitted to ING false identifying information for the insureds, such as false social security numbers. One of the Fifteen Insureds is a Confidential Informant ("CI1"). Liberty Planning submitted an application for a $10,000,000 life insurance policy on behalf of CI1. ING approved the CI1 application.

11. CI1 stated that in late 2007, CI2, who is CI1's accountant, contacted CI1 and told him that he knew someone named EDWARD GRODSKY who was looking for healthy elderly persons who were willing to purchase life insurance. According to CI2, he knew GRODSKY because GRODSKY was also an accountant who sold

---

[2]Insurance companies in general, and ING in particular, will not knowingly issue life insurance policies to persons who are "strangers" to the insured, that is, persons who have no interest in the continued health of the insured and to whom the insured is worth more dead than alive.

[3]Liberty Planning, in addition to submitting applications to ING for each of the Fifteen Insureds, also submitted, on behalf of many of the Fifteen Insureds, applications for life insurance coverage to life insurance companies other than ING.

accounting software to CI2. According to CI1, GRODSKY called CI1 and told him that: (1) CI1 could obtain life insurance since he was healthy and between the ages of 81 and 84; (2) "investors," whom GRODSKY did not otherwise identify, rather than CI1 himself, would be paying the premiums on this policy; (3) the policy would be resold after two years at which time CI1 would be paid $2 million; and (4) CI1 would be paid $500 per month until the policy was resold. According to CI1, GRODSKY later told CI1 that CI1's net worth would be inflated in his insurance application. CI1 told the government that, in fact, his net worth is "very little," that he rents his apartment, and that from social security and his pension his total annual income is about $36,000. CI2 spoke to the government, and in substance, confirmed the above facts. The CI1 life insurance application that Liberty Planning submitted to ING, shows that the net worth and annual income figures that Liberty Planning listed for CI1 on CI1's insurance application to ING were, respectively, $17,400,000 and $475,000. The completed applications which Liberty Planning submitted for CI1 falsely stated that CI1 had not had any discussions about reselling the policy and that the premiums were going to be paid from income and savings (when in fact, they were going to be paid, and were paid, by investors). According to CI2, CI2, at GRODSKY's direction, was made the trustee of the CI1 life insurance trust and the trust bank account paid the premiums. According to CI2, he signed a number of starter checks for the trust bank account in blank at

GRODSKY's direction, but otherwise played no part in making deposits into or disbursing funds from this bank account. A review of bank records show that the trust bank account was funded by organizations of which CI2 stated that he had never heard, including a company called the Blue Rock Group. Bank records show that the Blue Rock Group also made $500 monthly payments to CI1 for five months. Based upon my investigation thus far, I believe that the Blue Rock Group, which appears to be funded by Bold Associates, is controlled by EDWARD GRODSKY and other coconspirators. Further, records show that MOSES NEUMAN, YUDAH NEUMAN, and GRODSKY are the trustees of numerous insurance trusts' bank accounts purportedly opened and funded by the insureds and/or its beneficiaries, but investigation revealed that the co-conspirators were indeed the ones who controlled the insurance trusts' bank accounts.

12. Thereafter, CI2 and GRODSKY engaged in several email exchanges, copies of which CI2 provided, including, among others, the following:

a. On or about January 28, 2008, GRODSKY sent an email, not from the PREMISES, but from his office email address, to CI2 stating: "Could you do me a favor and sign the attached and then fax it back to me at 646-349-3805. Thanks, Ed[.] EG Systems, Inc. 3334 Long Beach Road, Suite 160, Oceanside, NY 11572 (800) 264-3155 voice (646) 349-3805 fax http://www.w21099.com//"). The subject line of the email was the name of CI1. In response to GRODSKY's email, CI2 signed the

attachment, an insurance document titled "Life Application State Verification" from Phoenix Life Insurance Company. On or about January 28, 2008, CI2 sent the signed Life Application form to GRODSKY via fax.

b. On or about February 12, 2008, GRODSKY sent an email from the PREMISES to CI2 stating: "Please download the attached form and fax it back to me at the number below. Ed[.] EG Systems, Inc., 3334 Long Beach Road, Suite 160, Oceanside, NY 11572 (800) 264-3155 voice (646) 349-3805 fax http://www.w21099.com//"). In response to GRODSKY's email, CI2 signed the attachment, an insurance document titled "Financial Information", which falsely listed the "Estimated Net Worth" of CI1 in the amount of $17,400,000. The Financial Information form also contained a false breakdown of CI1's annual income which totaled $750,000 and a false breakdown of CI1's liabilities which totaled to "$100K". On or about February 12, 2008, CI2 returned the Financial Information form to GRODSKY via fax with the signatures of CI1 and CI2.

c. On or about February 14, 2008, GRODSKY sent an email to CI2 from the PREMISES stating: "The attached is a signed doc from "[CI's first name]". Please sign and fax back to me at the number below. Thanks, Ed (646) 349-3805 fax". It is believed the word "[CI's first name]" referred to CI1. In response to GRODSKY's email, CI2 signed the attached insurance document titled "Life Application State Verification" from Phoenix Life Insurance Company. On or about February 14, 2008,

CI2 sent the Life Application form to GRODSKY via fax with the signatures of CI1 and CI2.

d. Below the above mentioned message on February 14, 2008, there were two forwarded messages between the PREMISES and CI1. The first forwarded message was dated on or about February 13, 2008, which showed that GRODSKY sent an email to CI1 stating: "Please sign and return to me. If you can't open it, let me know and I will fax it. Sign where it says insured. Regards, Ed" The second forwarded message was dated on or about February 13, 2008 from CI1 responding to an earlier GRODSKY email stating: "...look O.K.? Regards, [CI1]"

e. On or about February 19, 2008, GRODSKY sent an email from the PREMISES to CI2 stating: "Please sign and fax back to me at 646.349.3805. Ed" In response to GRODSKY's email, CI2 signed the attached insurance document titled "Financial Information (Continued)", which listed five questions to be answered by the insured or owner of the proposed insurance policy with ING. On or about February 19, 2008, CI2 returned the Financial Information form to GRODSKY via fax with the signatures of CI1 and CI2. Although the form was signed by CI1 and CI2, all five questions on the form were unanswered.

f. On or about March 13, 2008, GRODSKY sent an email with an attachment from the PREMISES to CI2 stating: "Please sign and fax back to 718-301-9051 today. Thanks, Ed Grodsky." In response to GRODSKY's email, CI2 signed the attached insurance documents titled "Numeric Summary", which

illustrated different death benefit payout options concerning CI1's fraudulent policy with ING. The document also showed AVIGDOR GUTWEIN, a Liberty Planning agent, as the insurance agent of the policy, even though neither CI1 nor CI2 have ever met GUTWEIN. In addition, CI2 also signed another insurance document of what appeared to be the last page of some sort of agreement. On or about March 13, 2008, CI2 sent the signed Numeric Summary and the signature page of the agreement document to GRODSKY via fax.

g. On or about March 18, 2008, GRODSKY sent an email with an attachment from the PREMISES to CI2 stating: "Please sign and fax back to me at the number below. Thanks, Ed" In response to GRODSKY's email, CI2 signed the attached insurance document titled "Numeric Summary," which illustrated different death benefit payout options concerning CI1's fraudulent policy with ING. This document is similar to the document mentioned in the previous paragraph but has a different signature date. The document also showed GUTWEIN as the insurance agent of the policy. On or about March 18, 2008, CI2 sent the Numeric Summary to GRODSKY via fax.

h. On or about January 21, 2010, GRODSKY sent an email with an attachment from the PREMISES to CI2 stating: "Please review and send back to me. You can either fax or scan. Ed[.] EG Systems, Inc., 3334 Long Beach Road, Suite 160, Oceanside, NY 11572 (800) 264-3155 voice (646) 349-3805 fax[.] [The PREMISES]"). The subject line of the email was "[CI] papers

to be signed". The attachment is an insurance document titled "Surrender Application" from ING.

i. On or about January 21, 2010, GRODSKY sent an email from the PREMISES to CI2 stating: "The form you are signing is not going to be submitted. It will be held just in case ING starts something. Ed".

CONSENSUAL MONITORED CALLS

13. On December 22, 2009, CI2 telephoned GRODSKY after GRODSKY left a voice mail at CI2's answering machine and requested CI2 to call him. During the consensually monitored telephone call, GRODSKY informed CI2 that ING was in the processing of cancelling insurance policies sold through Liberty Planning and CI2 might be served with summons issued by the insurance company. GRODSKY directed CI2 that when and if CI2 received the summons, "You'll email me the papers, okay." GRODSKY further discussed the fraudulent scheme with CI2, and, among other things, the following discussions took place:

a. GRODSKY advised CI2 that although the insurance trusts' bank accounts have been closed, the investors are still paying premiums on the fraudulent policies;

b. When GRODSKY was asked by CI2 whether CI1 needed to be not healthy, now that they are ready to sell the CI1 policy, GRODSKY responded, "Well, if you want to increase the value of this yeah, you can go for not healthy. If you really want to play it out, you can make more money that way";

c. GRODSKY advised CI2 that CI2 will definitely earn some monies for his role in the scheme, and they may advise CI1 to revisit the doctor a few more times. I believe that GRODSKY wanted to have potential buyers of the policy believe that CI1's health is worse than it actually is.

14. On December 30, 2009, CI1 telephoned GRODSKY after GRODSKY left a voice mail at CI1's answering machine and requested CI1 to call him. During the consensually monitored telephone call, CI1 expressed concern to GRODSKY that false information had been placed on his insurance application, namely, the false statement that his company was worth a couple of million dollars. GRODSKY stated, "Stop questioning the assets. They don't like it when somebody else gives you money to buy insurance." During the same telephone call, GRODSKY advised CI1, "It's a policy and it's gonna sell and you'll, hopefully you'll make some money out of it. But if you want to maximize the money the less healthy you are the better it is. That's the way these things work."

TITLE III INTERCEPTION

15. Commencing on January 20, 2010, the Investigating Agencies have been intercepting wire communications on the cellular telephone of MOSES NEUMAN, as authorized in an order issued pursuant to 18 U.S.C. § 2518 by the Honorable Sandra L. Townes. Among the telephone calls intercepted, GRODSKY had the following discussions with NEUMAN:

a. On or about January 20, 2010, GRODSKY told NEUMAN, "tell your brother he has to send me that email again."

b. On or about January 25, 2010, GRODSKY told NEUMAN that there was an insurance broker who might be interested in purchasing insurance policies. GRODSKY stated, "I'll email it [the broker's telephone number] to you. Just listen, just talk to him. That's all, he's a nice guy. Okay?" During the intercepted telephone calls, NEUMAN reminded GRODSKY numerous times to send this insurance broker's telephone number to him via email.

CONCLUSION

16. Based upon the information set forth above there is probable cause to believe that on the computer systems owned, maintained, and/or operated by AOL, there exists evidence, fruits and instrumentalities of violations of Title 18, United States Code, Sections 371, 1341, 1343, 1349 and 1956. By this affidavit and application, I request that the Court issue a search warrant directed to AOL allowing Agents of the Investigating Agencies to seize email and other information stored on the AOL servers for the computer account and files specified in Attachment A. The warrant will be faxed to AOL personnel who will be directed to produce those accounts and files.

18. As this investigation is continuing, disclosure of the search warrant, this affidavit, and/or this application and the attachments thereto will seriously jeopardize the investigation. Accordingly, I request that the Court issue an

order that the search warrant, this affidavit in support of the application for a search warrant, the application for a search warrant, and all attachments thereto be filed under seal until further order of the Court. In addition, because notification of the existence of this order will seriously jeopardize an investigation, I request the Court issue an order pursuant to 18 U.S.C. Section 2705(b) ordering AOL not to notify any person of the existence of the warrant.

SEARCH PROCEDURE FOR THE PREMISES

19. In order to ensure that agents search only those computer accounts and/or files described in Attachment A, this affidavit and application for a search warrant seek authorization to permit employees of the Provider to assist agents in the execution of this warrant. The search warrant will be faxed to AOL personnel who will be directed to produce those accounts and files described in Section II of Attachment A.

WHEREFORE, I respectfully request that a search warrant issue, pursuant to Rule 41 of the Federal Rules of Criminal Procedure and 18 U.S.C. § 2703(a), authorizing agents of the Investigative Agencies, to search the contents of the PREMISES KNOWN AS ELECTRICAL MAIL ADDRESS "EGSYS@AOL.COM" controlled by the web-based electronic mail service provider America Online, authorizing Special Agents of the Investigative Agencies to seize

ST
concerning the participation
the items described in Attachment A, ~~all of which constitute~~
of EDWARD GRODSKY in a scheme to commit
~~evidence, fruits and instrumentalities of~~ violations of Title 18,

United States Code, Sections 371, 1341, 1343, 1349 and 1956.

Dated: February 5, 2010
Brooklyn, New York

Sheldon Tang
Special Agent
Internal Revenue Service

Sworn to before me this
5 day of February, 2010

UNITED STATES MAGISTRATE JUDGE
EASTERN DISTRICT OF NEW YORK

ATTACHMENT A

I. Search Procedure

The search warrant will be faxed to Provider personnel who will be directed to produce those accounts and files described in Section II below.

II. Files and Accounts to be Produced

For the period from January 1, 2008 ST to the present:

a. All stored electronic mail and other stored content information presently contained in, or on behalf of, the AOL and AOL Instant Messenger account for the email address EGSYS@aol.com (hereinafter, the "Account");

b. All histories, profiles and "buddy lists" and/or "Friends lists" (including electronic mail addresses, screen names and/or ID's and other information stored) associated with the Account described above in Section II(a);

c. All existing printouts from original storage of all of the electronic mail described above in Section II(a);

d. All transactional information of all activity of the Account described above in Section II(a), including log files, dates, times, methods of connecting, ports, dial-ups, and/or locations;

e. All business records and subscriber information, in any form kept, pertaining to the Account described above in

Section II(a), including applications, subscribers' full names, dates of birth, social security numbers, all screen names associated with the subscribers and/or accounts, all account names associated with the subscribers, methods of payment, telephone numbers, addresses, and detailed billing records;

f. All records indicating the services available to subscribers of the Account described above in Section II(a); and

g. All email, including any attachments, sent by or received by the Account described above in Section II(a), whether saved or deleted, whether contained in the email accounts or in a customized "folder";

h. All instant messenger messages, calendar items, screen names, member profiles, contacts, buddy lists and the content of any AOL online account features such as AOL pictures and Xdrive storage maintained by, or related to the Account described above in Section II(a).

I. All web-pages, including any associated links, that were created or maintained by the user(s) of the Account described above in Section II(a).

ST

III. The items above will be produced ~~the~~ to taint Agents, not connected with this Investigation, to make sure that only items that concern the participation of EDWARD GRODSKY in ~~violation~~ a scheme to commit conspiracy, mail fraud, wire fraud and money laundering in violation of Title 18, United States Code, Sections 371, 1341, 1343, 1349 and 1956 are produced to the Investigating Agents and the prosecution team.